AFRL-HE-AZ-TP-2002-0004

UNITED STATES AIR FORCE RESEARCH LABORATORY

DEVELOPMENT OF COMPUTER-GENERATED FORCES FOR AIR FORCE SECURITY FORCES DISTRIBUTED MISSION TRAINING

Joseph L. Weeks

Air Force Research Laboratory
Warfighter Training Research Division
6030 South Kent Street
Mesa, AZ 85212-6061

L. Bruce McDonald
Jack Hughes

McDonald Research Associates, Inc.
120 University Park Dr.
Winter Park, FL 32792

October 2002

AIR FORCE MATERIAL COMMAND
AIR FORCE RESEARCH LABORATORY
HUMAN EFFECTIVENESS DIRECTORATE
Warfighter Training Research Division
6030 South Kent Street
Mesa AZ 85212-6061

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
01-10-2002	Interim	xx-01-2001 to xx-12-2001

4. TITLE AND SUBTITLE
Development of Computer-Generated Forces for Air Force Security Forces Distributed Mission Training
Unclassified

5a. CONTRACT NUMBER
F41624-97-D-5000

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
62205F

6. AUTHOR(S)
Weeks, Joseph L. ; Author
McDonald, L. Bruce ; Author
Hughes, Jack ;

5d. PROJECT NUMBER
4924

5e. TASK NUMBER
B2

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Air Force Research Laboratory
Warfighter Training Research Division
6030 South Kent Street
Mesa, AZ85212-6061

8. PERFORMING ORGANIZATION REPORT NUMBER
AFRL-HE-AZ-TP-2002-0004

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
Air Force Research Laboratory
Warfighter Training Research Division
6030 South Kent Street
Mesa, AZ85212-6061

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL; AFRL/HEA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES
Air Force Research Laboratory Technical Monitor: Dr Joseph L. Weeks, 480.988.6561 x-249, DSN 474-6249. This documents a presentation at the 2001 Interservice/Industry Training, Simulation, and Education Conference, held 26-29 Nov 01, held in Orlando FL.

14. ABSTRACT
This paper describes the Computer-Generated Forces (CGF) behavior development on the Air Force Research Laboratory Security Forces Distributed Mission Training (SecForDMT) technology development program. The near-term goal of this program is to develop distributed training technology that will allow Air Force Security Force decision-makers to practice planning and execution of air base defense. The system must be distributed because Air Force Security Forces are drawn from many separate home bases and receive limited training as a team before deployment to a contingency site. The training target is the decision-makers as opposed to the trigger pullers in the fire teams. This emphasis on decision-makers is because needs assessments have indicated training requirements for these positions. We will use CGFs to simulate fire team members, other friendlies, neutrals and threats to generate situations requiring decisions by the trainees. The CGFs being developed on this project are different from other CGFs in a number of ways. Security forces CGFs challenge, engage, or capture threat CGFs in accordance with the rules of engagement stated in the trainee-generated OPORD as well as level of compliance by OPFOR CGFs. Since these CGFs will be controlled directly by the trainees instead of an experienced CGF master, a simple, understandable user interface is a major design requirement. This paper discusses the process of defining behaviors for computer-generated forces and how these behaviors were implemented. It also discusses initial evaluations of behaviors, lessons learned, and future plans for extending and improving these behaviors.

15. SUBJECT TERMS
Air base defense; Behavior development; CGF; Computer-generated forces; Distributed Mission Training; Distributed training technology; DMT; Force protection; SecFor DMT; Security Forces; Security Forces Distributed Mission Training; Training

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	18	Casey, Liz liz.casey@williams.af.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 480988-6561 DSN 474-6188

NOTICES

Publication of this papter does not constitute approval or disapproval of the ideas or findings. It is published in the interest of STINFO exchange.

Using Government drawings, specifications, or other data included in this document for any purpose other than Government-related procurement does not in any way obligate the US Government. The fact that the Government formulated or supplied the drawings, specifications, or other data, does not license the holder or any other person or corporation, or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

The Office of Public Affairs has reviewed this paper, and it is releasable to the National Technical Information Service, where it will be available to the general public, including foreign nationals.

This paper has been reviewed and is approved for publication.

JOSEPH L. WEEKS
Project Scientist

DEE H. ANDREWS
Technical Advisor

CURTIS J. PAPKE, Colonel, USAF
Chief, Warfighter Training Research Division

Copies of this report may be requested from:

Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Ft. Belvoir, VA 22060-6218
http://stinet.dtic.mil

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
October 2002	Interim	Jan 01 to Dec 01

4. TITLE AND SUBTITLE

Development of Computer-Generated Forces for Air Force Security Forces Distributed Mission Training

5a. CONTRACT NUMBER
F41624-97-D-5000

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
62205F

6. AUTHOR(S)

Joseph L. Weeks, L. Bruce McDonald, Jack Hughes

5d. PROJECT NUMBER
4924

5e. TASK NUMBER
B2

5f. WORK UNIT NUMBER
06

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory
Human Effectiveness Directorate
Warfighter Training Research Division
6030 South Kent Street
Mesa AZ 85212-6061

McDonald Research Associates, Inc.
120 University Park Dr.
Winter Park, FL 32792

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory
Human Effectiveness Directorate
Warfighter Training Research Division
6030 South Kent Street
Mesa AZ 85212-6061

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-HE-AZ-TP-2002-0004

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Air Force Research Laboratory Technical Monitor: Dr Joseph L. Weeks, 480.988.6561 x-249, DSN 474-6249. This documents a presentation at the 2001 Interservice/Industry Training, Simulation, and Education Conference, held 26-29 Nov 01, held in Orlando FL.

14. ABSTRACT This paper describes the Computer-Generated Forces (CGF) behavior development on the Air Force Research Laboratory Security Forces Distributed Mission Training (SecForDMT) technology development program. The near-term goal of this program is to develop distributed training technology that will allow Air Force Security Force decision-makers to practice planning and execution of air base defense. The system must be distributed because Air Force Security Forces are drawn from many separate home bases and receive limited training as a team before deployment to a contingency site. The training target is the decision-makers as opposed to the trigger pullers in the fire teams. This emphasis on decision-makers is because needs assessments have indicated training requirements for these positions. We will use CGFs to simulate fire team members, other friendlies, neutrals and threats to generate situations requiring decisions by the trainees. The CGFs being developed on this project are different from other CGFs in a number of ways. Security forces CGFs challenge, engage, or capture threat CGFs in accordance with the rules of engagement stated in the trainee-generated OPORD as well as level of compliance by OPFOR CGFs. Since these CGFs will be controlled directly by the trainees instead of an experienced CGF master, a simple, understandable user interface is a major design requirement. This paper discusses the process of defining behaviors for computer-generated forces and how these behaviors were implemented. It also discusses initial evaluations of behaviors, lessons learned, and future plans for extending and improving these behaviors.

15. SUBJECT TERMS

Air base defense; Behavior development; CGF; Computer-generated forces; Distributed Mission Training; Distributed training technology; DMT; Force protection; SecFor DMT; Security Forces; Security Forces Distributed Mission Training; Training

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Liz oCasey
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED	18	19b. TELEPHONE NUMBER *(include area code)* 480.988.6561 x-188 DSN 474-6188

PREFACE

This research was conducted for the Air Force Research Laboratory, Human Effectiveness Directorate, Warfighter Training Research Division (AFRL/HEA) under USAF Contract No. F41624-97-D-5000, and Work Unit 4924B206, Force Protection: Distributed Mission Training. The Laboratory Technical Monitor was Dr Joseph L. Weeks, AFRL/HEA.

This documents a presentation at the 2001 Interservice/Industry Training, Simulation, and Education Conference, held 26-29 Nov 01, held in Orlando FL.

DEVELOPMENT OF COMPUTER GENERATED FORCES FOR AIR FORCE SECURITY FORCES DISTRIBUTED MISSION TRAINING

Bruce McDonald, Ph.D.*
Joseph Weeks, Ph.D.**
Jack Hughes*
* McDonald Research Associates
Winter Park, Florida
** Air Force Research Laboratory
Warfighter Training Research Division
Mesa, Arizona

Abstract

This paper describes the Computer Generated Forces (CGF) behavior development on the Air Force Research Laboratory Security Forces Distributed Mission Training (SecForDMT) technology development program. The near-term goal of this program is to develop distributed training technology that will allow Air Force Security Force decision-makers to practice the planning and execution of air base defense. The system must be distributed because Air Force Security Forces are drawn from many separate home bases, and receive only limited training as a team before deployment to a contingency site. The training target is the decision-makers (e.g. Squad Leaders, Flight Leaders, S-3, Base Defense Commander) as opposed to the trigger pullers in the fire teams. This emphasis on decision-makers is due to the fact that needs assessments have indicated training requirements for these positions. We will use CGFs to simulate fire team members, other friendlies, neutrals and threats in order to generate situations requiring decisions by the trainees.

The CGFs being developed on this project are different from other CGFs in a number of ways. These CGFs do not exhibit cold war behavior of always fighting to the death. Although opposing force (OPFOR) CGFs are capable of lethal force, they do not automatically shoot given intervisibilty. Neutral CGFs are capable of a range of behaviors varying from peaceful intent to lethal threat. Security Forces CGFs who observe such threats issue doctrinally correct situation reports (SITREPs) for students' situational assessment, decision making, and operations order/fragmentary order (OPORD/FRAGO) formulation. Security forces CGFs challenge, engage, or capture threat CGFs in accordance with the rules of engagement (ROE) stated in the trainee-generated OPORD as well as level of compliance by OPFOR CGFs. Since these CGFs will be controlled directly by the trainees instead of an experienced CGF master, a simple, understandable user interface is a major design requirement. This paper discusses the process of defining behaviors for computer generated forces and how these behaviors were implemented. It also discusses initial evaluations of behaviors, lessons learned and future plans for extending and improving these behaviors.

Biographical Sketch:

BRUCE MCDONALD holds a Ph.D. in Industrial Engineering from Texas A&M University and has 25 years experience in R&D, analysis, design and production of simulation and training systems. He is currently the Principal Investigator on the Security Forces Distributed Mission Training Technology (SecForDMT) program. Dr. McDonald was the Principal Investigator on a DARPA/STRICOM/DMSO program to develop the DIS Standards and served as chair of the DIS Steering Committee. He has conducted research projects on the development of correlation measures between environment models in separate host computers, improved dead reckoning equations, and the development of computer generated forces with electronic warfare simulation capabilities. Dr. McDonald was the chair of the DIS Standards Coordinating Committee Special Task Group on High Level Architecture (STGHLA). He has performed requirements analyses on the Battle Force Tactical Trainer and was the Program Engineer on the Catapult Launch Systems Trainer program. His strengths are in modeling and simulation R&D, primarily in the areas of user needs assessment, concept formulation, requirements analysis, CGF development, fidelity requirements, behavioral representation, interoperability analysis, and distributed simulation state-of-the-art.

JOSEPH WEEKS currently serves as lead scientist for security forces training initiatives at the Air Force Research Laboratory (AFRL). He has 25 years of experience as a research psychologist working in the areas of manpower, personnel and training. He has conducted research into procedures for quantifying occupational learning difficulty, procedures for using learning difficulty to determine job qualification requirements, learning abilities measurement and the impact of individual differences on student performance in undergraduate flying training. From 1988 to 1998, he served as branch chief responsible for supervision of scientific and technical personnel and management of a million-dollar, annual contract research budget. In 1998, he was assigned to the Warfighter Training Research Division where he independently conducted a study of operator qualification requirements for DoD unmanned aerial vehicles. His research interests include acquisition of expertise in decision making and effectiveness of simulation training. He holds a Ph.D. in Educational Psychology from the University of Texas.

JACK HUGHES holds BS degrees in both Computer Science and Physics from the University of Central Florida. He is the lead software engineer on the SecForDMT program, where he is responsible for design, development and testing of the required CGF behaviors. Prior to joining MRA, he conducted research on Modular Semi-Automated Forces (ModSAF). Mr. Hughes is a Navy veteran and has experience in technical training.

DEVELOPMENT OF COMPUTER GENERATED FORCES FOR AIR FORCE SECURITY FORCES DISTRIBUTED MISSION TRAINING

Bruce McDonald, Ph.D.*
Joseph Weeks, Ph.D.**
Jack Hughes*
***McDonald Research Associates**
Winter Park, Florida
****Air Force Research Laboratory**
Warfighter Training Research Division
Mesa, Arizona

INTRODUCTION

In support of national military strategy, the USAF has adopted an Expeditionary Aerospace Force (EAF) concept for providing light, lean and lethal force packages consisting of combat and combat support elements tailored for specific global commitments. The personnel and equipment that implement this EAF concept are referred to as Aerospace Expeditionary Forces (AEF). Plans for AEF deployment call for the creation of Air Expeditionary Wings (AEWs) consisting of combat and combat support elements. These AEWs will be on alert to respond quickly to contingencies as tasked by the Joint Chiefs of Staff. Elements of AEWs would be created from forces located at geographically-separated locations. Once notified of a mission, these disparate combat and combat support units would deploy to a contingency site with minimal time available for training as a unit.

Limited Training Opportunities

One of the critical combat support elements is security forces. Security forces represent one of the largest active duty, career fields in the USAF consisting of 22,510 enlisted personnel and 861 officers ("Air Force Personnel Center; Personnel Statistics", 2001). Security forces ensure USAF combat capability through providing the functions of security for resources, installations and weapons systems; force protection; air base defense; military police services; information, personnel and industrial security; military working dog activities; and combat arms ("Security Forces Officer Specialty, Career Field Education and Training Plan", 2001).

Although all duties performed by security forces are critical for ensuring combat capability, air base defense has been the center of attention for defense analysts. Vick (1995) and Shlapak and Vick (1995) emphasize the centrality of aerospace power to national security strategy and the vulnerability of aerospace assets to ground attack. Their reports "Snakes in the Eagle's Nest" (Vick, 1995) and "Check Six Begins on the Ground" (Shlapak & Vick,1995) are primary training references for identifying significant events in USAF security forces history ("Security Forces Officer Specialty, Career Field Education and Training Plan", 2001).

Vick (1995) reviews the history of air base defense by focusing on World War II and Viet Nam. He concludes that, " Most large - unit attacks on airfields succeeded because defending ground forces were outnumbered, outgunned, or outclassed …shortages in high-quality rear-area security forces and a lack of surveillance assets were the most common weaknesses." (Vick, 1995).

Shlapak and Vick (1995) describe strategies for responding to the ground threat. They refer to penetrating and standoff attacks. Penetrating attacks consist of small teams breaking through the defensive perimeter to place bombs on aircraft and material. Standoff attacks consist of firing on aircraft, facilities, and personnel from a distance of several kilometers. They predict increased use of standoff attacks and indicate that "*without a serious effort to improve U.S. abilities to detect and counter standoff attacks, the USAF is likely to lose high-value aircraft or have base operations otherwise disrupted in some future conflict.*", (Shlapak & Vick, 1995). They recommend several strategies for countering this threat:

> "*Detect and defeat* the adversary outside the wire, *before it launches the attack*. Doing so requires surveillance of the entire area from which attacks could be launched, which could be achieved by implementing

> options that include …. - improving SP [security police] training – both individual and unit – for off-base operations." (Shlapak & Vick, 1995).

Current training for security forces includes off base operations. Reconnaissance and combat patrol operations are taught during enlisted and officers training for ground combat skills. In addition, security forces personnel assigned to deployable positions are required to attend regional centers for sustainment training once every three years. Sustainment training includes instruction for reconnaissance and combat patrol operations. It appears that training for off-base operations could be improved by increasing the frequency of training. Anecdotal reports from USAF ground combat skills instructors indicate that security forces simply do not have the opportunity to practice their skills often enough (McDonald & Weeks, 2000).

To obtain more information to determine if a training gap exists and to identify tasks that should be emphasized during training, a security forces officer training needs survey was conducted via the world wide web. The survey resulted in a valuable empirical data base for indicating training needs. The sample of participants represented 46% of active duty security forces officers. These officers suggest that a training gap does exist in the domain of air base defense. They recommend training for personnel at the flight level more frequently than once every three years and made specific recommendations about the air base defense tasks that should be emphasized during training. Results from this survey are documented by Weeks, Garza, Archuleta, and McDonald (2001).

SecForDMT PROGRAM

An AFRL project has been initiated to determine strategies for affordable distributed mission training for security forces (McDonald, Weeks and Harris, 2000). The project is known as Security Forces Distributed Mission Training or SecForDMT. The current approach consists of design, development, and evaluation of interactive simulations via the Internet. Early assessments of this technology indicated great potential for the support of training in decision making, and team coordination.

Figure 1 is a Security Forces Flight, which generally consists of a leadership element and three squads. The

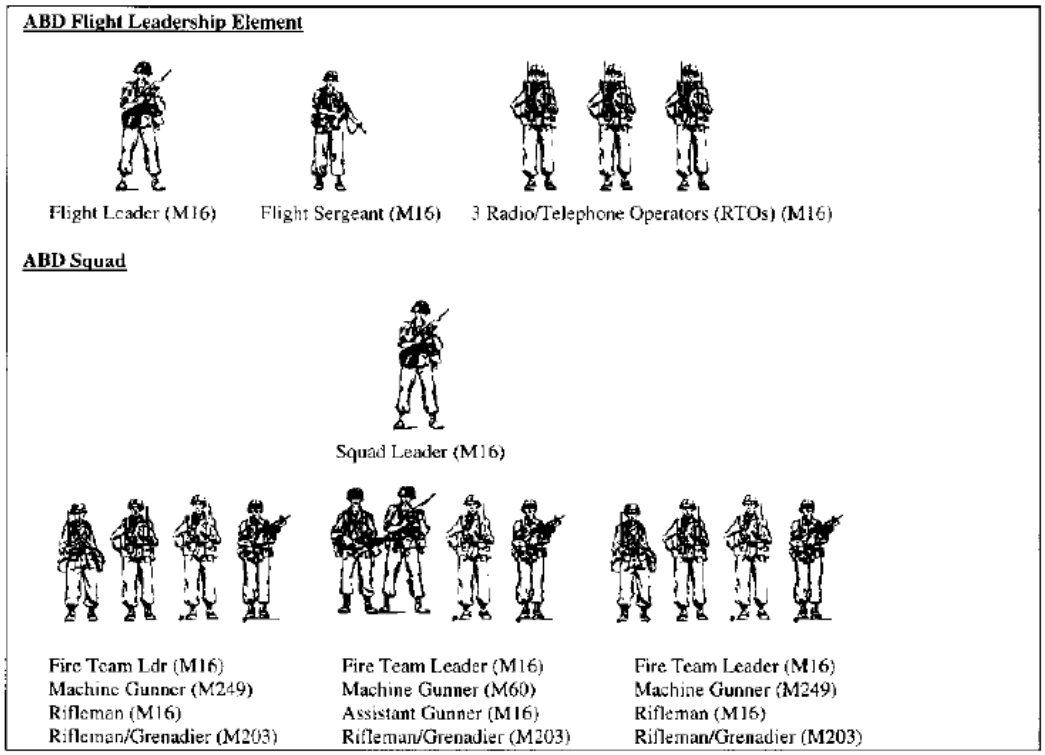

Figure 1
Security Forces Flight

Security Forces Flight is the basic element of air base defense and is modeled after a Marine Platoon.

Goal

The goal of the SecForDMT program is to provide Air Force Security Forces with a tool to train decision-makers how to plan and execute air base defense missions while still located at their home stations. This tool will allow decision-makers to maintain their skills between training rotations at the regional training centers once every three years. It will also allow security force members of an AEW to learn how to work as a team before deployment.

Operational Concept

Figure 2 illustrates our proposed training system technology test bed. The instructor and trainee stations will communicate over the Internet or a local area network depending on the locations of the trainees and instructor. This communication will be DIS/HLA compliant. The system is designed as a learning environment for leadership and decision-making (squad leader to flight leader) as opposed to trigger pulling. Friendly fire teams, OPFOR and non-combatants will be modeled with computer generated forces (CGFs). The flight leader and flight sergeant will communicate with the squad leaders via simulated tactical radio/telephone messages over the Internet. If desired, additional layers may be added up to the base defense operations center (BDOC).

When the instructor selects an exercise, the trainees will be notified to review the matching Operations Order (OPORD) on the screen or print out the MS Word document. The flight leader will use the resources contained in the OPORD and prepare a plan for defending the assigned sector. This plan will be incorporated into a more detailed OPORD which is transmitted to squad leaders via email. The OPORD would contain squad missions, intelligence and Rules of Engagement (ROEs). Squad leaders would then use simple menu entries to select fire team personnel in the form of CGFs, assign weapons and sensors to them and place fire teams in battle positions. Squad leaders would use menu commands to set ROE in keeping with the OPORD. A more detailed description of the SecForDMT concept is contained in McDonald, et.al, (2000).

Technical Hurdles

The technical hurdles of this project may be grouped under three headings: Affordability, Validity and Usability. Each of these hurdles is discussed separately below.

Affordability

The first technical hurdle is affordability. Air Force Security Forces have extremely tight training budgets. During the problem definition phase of the project, Security Forces (SF) leaders informed us that any training system that could not be run on a standard (GSA Schedule) PC with limited memory and graphics enhancements was unlikely to be fielded in quantities sufficient to achieve the training goal. In addition, SF personnel will not have access to special high speed data lines. Consequently, the system must be designed to run over standard Internet access lines via 56K modems.

Validity

The next technical hurdle is to provide the trainees with the type of information they would receive in the real world as opposed to the omniscient views provided to video game players and computer generated forces controllers (CGFMasters). Most video games provide the player with an overhead view of opponent locations. Almost all CGF control stations are designed for CGFMasters, who must know where all of the friendlies and threats are located in order to do their jobs properly. In a real world base defense scenario, the threats, friendlies and neutrals will be detected by fire team members because they are located forward. The decision-makers generally find out about activities in their sector through SPOT Reports generated by the fire team members. Even when on patrol, FM 7-8 states that a fire team should take the point ahead of the squad leader. Consequently, decision-makers must be trained to rely on SPOT Reports from their fire teams as their primary means of detecting activities in their sector.

Another issue is that video games and most CGFMaster stations will allow the user to move the stealth display eye point to any desired location. In the real world, the SF decision-makers are limited to the view at their present location and moving to another location entails time delays. SecForDMT is being designed to limit trainee views to those available in the real world.

Finally, the average computer monitor cannot display sufficient resolution to allow a trainee to detect, recognize and identify targets at ranges achievable in the real world. Consequently, if detection ranges are properly modeled, CGFs will be able to detect targets well beyond the ranges at which humans can detect these same targets on stealth displays. This mismatch in detection ranges has lead to fair fight issues in mixed

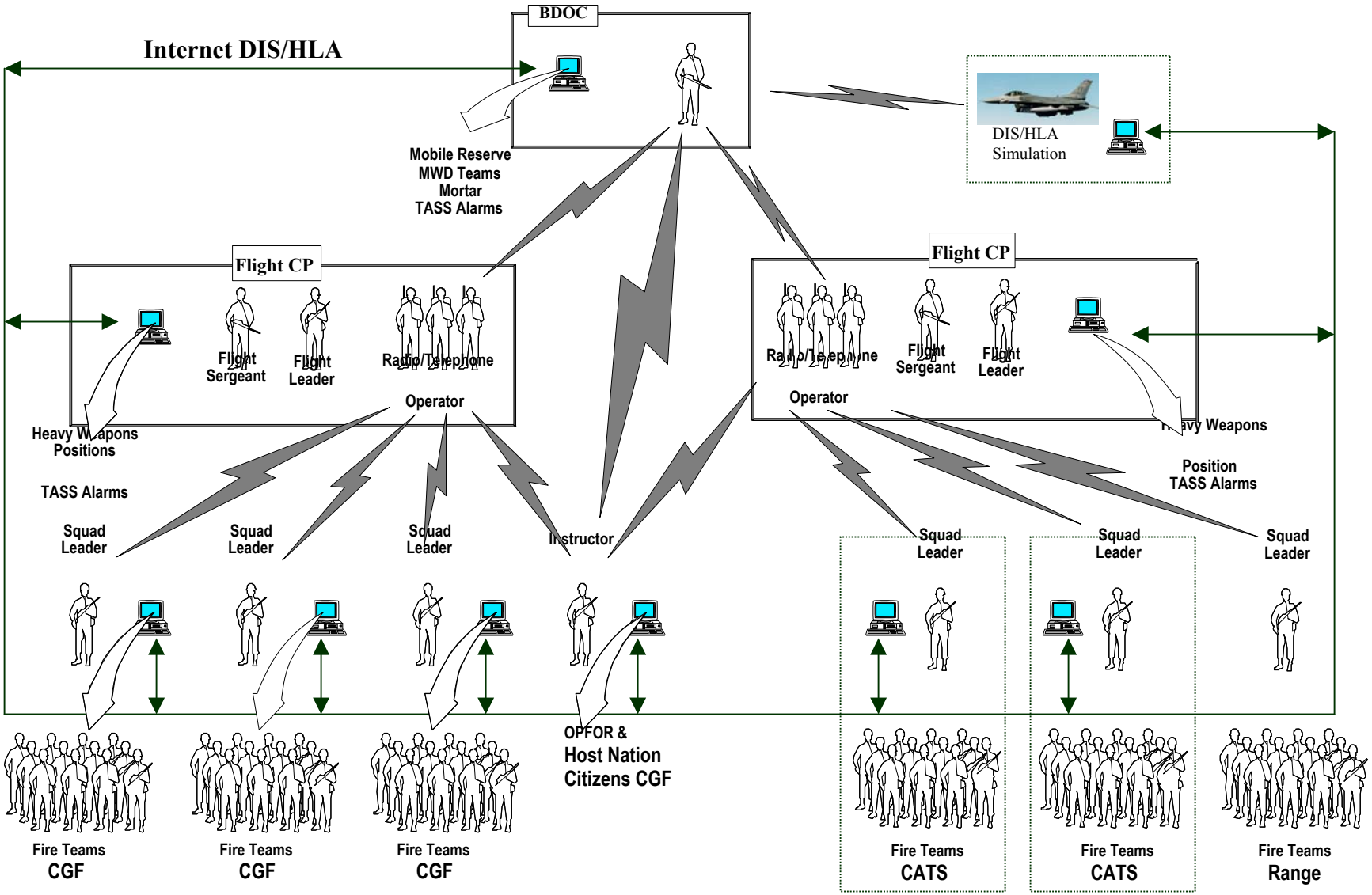

Figure 2
SecForDMT Concept

constructive/virtual simulations. If you degrade detection capabilities of CGFs to match that of humans using stealth displays, then the performance of the CGFs will no longer represent real world capabilities, leading to negative training. While this problem is not as apparent in close battle situations such as urban environments, it is very critical in the average air base defense scenario in which stand off distance is a major objective in defense planning. As a general rule, table top displays lag behind the capabilities of high fidelity flight simulators by several years. Since high fidelity flight simulators have not yet achieved 20/20 vision, it will be a number of years before standard computer displays can match real world performance. This mismatch between human and CGF target detection capabilities must be addressed in the development of SecForDMT technology.

Usability

In order for SecForDMT technology to be cost effective, trainees must (1) control the CGFs directly without the aid of a CGFMaster and (2) be able to begin training after only a short introduction to the user interface. Almost all CGFMaster user interfaces fail this test. The flexibility and power of most CGFMaster interfaces leads to an intimidating interface that takes months to master. If the SecForDMT technology development effort used an unmodified CGFMaster user interface, there is the danger that the trainees would become CGF control experts as opposed to security forces decision-making experts. The SecForDMT technology development effort has established a goal that squad leaders and officers will be able to conduct productive training after one half hour of user interface familiarization.

Approaches

The approaches used in the first phase of the SecForDMT project are discussed under the headings of Computer Generated Forces, and Initial Emphasis.

Computer Generated Forces

As stated above, fire teams, will be simulated in SecForDMT. There are a number of alternative computer generated forces (CGFs) available for fulfilling this task. The primary considerations are that the CGFs provide valid simulations of fire team behaviors and that they be easy for instructors and squad leaders to operate. The authors evaluated the strengths and weaknesses of JCATS, ITEMS, ModSAF and VR-Forces. JCATS simulates individual combatants but has evolved from Janus, which is optimized for platoons and above. Since it was initially designed for use by Operations Research Analysts, the user interface is too complex to be mastered in a short period of time by a trainee. The National Research Council report on Modeling Human and Organizational Behavior states that "Currently, no human behavior representation is included [in JCATS], and all tactics and play are specified by the human players"(Pew and Mavor, 1998). It was decided that JCATS would require too much detailed control by trainees and divert them from their learning objectives. ITEMS does not currently model individual combatants and a decision was made that creating this capability would require too many project resources. ModSAF was originally designed for training rather than analytical applications and the DISAF variant supports simulation of individual combatants. These computer generated entities can execute a number of rudimentary commands and fairly complex behaviors can be developed by the use of scripts. A drawback to ModSAF is that it has evolved over a number of years and the code is complex and difficult to understand. The CGF community is evolving toward the development of OneSAF which will base much of its functionality on ModSAF. Once OneSAF matures, it will be an extremely powerful tool. However, a decision was made that OneSAF would not be mature enough to fulfill the goals of SecForDMT over the next several years. In addition, DISAF source code is not available, so project personnel would be unable to create the required behaviors such as challenge and surrender. VR-Forces is a newly developed Commercially available CGF tool similar to ModSAF. It does not currently have dismounted infantry behavior implemented, but does have a convenient application programmer interface for creating these behaviors along with simplified user interfaces. This tool was developed recently using strong object oriented design. Since this tool comes with support from its developer, the project staff decided it could create the desired behaviors and interfaces more quickly and easily with VR-Forces than with other CGF tools. A decision was made to use VR-Forces on SecForDMT in order to meet the project goals of demonstrating initial capabilities at the end of the first year.

Initial Emphasis

In order to produce a product at the end of the first year of the project, a decision was made to emphasize static base defense and defer patrols and convoys to the second year. Consequently, the first year's effort implemented the SF tasks in Table 1.

DEFINING REQUIRED CGF BEHAVIORS

CGF behavior requirements were derived from military manuals and subject-matter expert interviews.

Military Manuals

The first step in defining CGF behaviors was to review the manuals used by security force instructors in teaching tactics, techniques and procedures (TTPs). Air Force Security Forces TTPs are contained in AFI 31-301 and AFH 31-302. These documents refer to FM 7-8 and U.S. Army soldier skills manual as an official training reference. The principal investigator reviewed these manuals as well as Air Force SF curriculum material before interviewing subject matter experts.

Table 1
Capabilities Implemented in First Phase

- Instructor Tasks
  - Positioning assets (aircraft and facilities) inside base
  - Creating scenarios
    - Selecting friendly/hostile/neutral/host nation citizen humans & vehicles
    - Defining movement, weapons, aggressiveness, ROEs
  - Re-tasking CGFs during exercise
- Trainee Tasks
  - Positioning fighting positions around base perimeter
    - Placing simulated fire team members (by weapon type) in positions
    - Designating fields of fire and sectors of responsibility
  - Positioning sensors around base perimeter and in dead zones
  - Positioning Entry Control Points (ECPs)
    - Placing guards at ECPs
  - Defining movement, weapons, ROEs
  - Re-tasking CGFs during exercise

Subject Matter Expert Interviews

SME interviews were structured around the procedures contained in the military manuals. Initial questions confirmed that the instructors did in fact teach TTPs contained in the military manuals discussed above. However, the Air Force SF instructors pointed out that the procedures contained in these manuals are heavily oriented toward cold war operations against regular military forces as opposed to terrorists operating in areas occupied by host nation citizens and other neutrals. In addition, the procedures contained in FM7-8 tended to emphasize offensive operations where air base security is much more defense oriented. The majority of the interview questions involved obtaining further detail on exactly how air base defense tasks are conducted by SF personnel. The hardest part of the interviews involved defining the various Rules of Engagement and how SF personnel were expected to respond to each possible event under varying ROEs.

Documenting Required Behaviors

The next task was to document the SF behaviors in a form implementable in software. As expected, the behaviors taught by the instructors consisted of a series of procedures that are implemented under various conditions. For example,

> If your mission is A, the ROEs are X, the environment around you is Y and the OPFOR does Z, then execute procedure B.

These behaviors were documented in pseudo code as a series of If-Then statements. The principal investigator then returned to the school to go over the pseudo code with the instructors. These interviews uncovered a number of details and nuances (especially in the areas of ROE implementation) that had not been completely documented in the initial interviews. This second interview also served to document the contents of situation reports (SITREPs) under each possible set of conditions.

We also interviewed Air Force SF Combined Arms Training and Maintenance personnel to determine the effective range of each SF weapon as well as the capabilities in Table 2

Table 2
SF Weapon Performance

- Probability of hitting a target
  - At various ranges
  - Good/fair/poor marksman
  - Standing/kneeling/prone shooter
  - Weapon hand held/on bipod/on tripod
  - Standing/kneeling/prone target
  - Small/large vehicle
  - Shooter under/not under fire
- Probability of kill

IMPLEMENTING BEHAVIORS

Based on results of the requirements analyses, the SF/threat/friendly/neutral behaviors in Table 3 were implemented during the first phase. In addition, we modeled the capabilities in Table 4.

Technical Literature Review

A literature review was conducted to obtain detection/recognition/identification ranges for camouflaged vehicles and personnel. We also reviewed the literature on alternative means of implementing behaviors in CGFs.

Approach Selected

Since the TTPs provided by the subject matter experts consisted primarily of If-Then statements that defined a series of states and correct procedures, these were most easily described in state transition diagrams and implemented as finite state machines. This is the same approach that is used in ModSAF. Behaviors were implemented in Microsoft Visual C++.

Table 3
SF/Threat/Friendly/Neutral Behaviors Modeled

- Occupy fighting positions and entry control points
- Monitor assigned sector
- Detect/recognize/identify threats/friendlies/neutrals
- Issue SITREPS and LACE reports
- Challenge intruders in sector
- Use correct challenging procedures
- Apply minimal level of force required
- Apply ROEs
- Capture/engage intruders
  - At perimeter
  - After base penetration
- Hold fire when neutrals/friendlies in field of fire
- Execute base penetration plan
- Exhibit intruder aggressiveness level
- Use cover and concealment
- Apply intruder ROEs

Table 4
Sensor and Weapon Performance Modeled

- Security Sensors
  - Types, ranges, sensitivities
  - Sensor reports
- Weapons performance
  - Probability of hit and kill

Implementation Successes and Problems

This section discusses some of the successes and problems encountered during the first phase of the project.

Basic Modeling Approach

Using the state transitions and finite state machines approach, it was straightforward to implement the behaviors described in the manuals as amplified by the subject matter experts. Primitive behavior such as moving, shooting and casualty assessment were handled by the underling VR Forces model. However, since VR Forces models vehicles, we had to implement significant modifications to accommodate the differences in movement parameters and different posture states of dismounted infantry. Also, since security forces must evaluate the behaviors of threats, friendlies and neutrals, we had to modify the target list in VR Forces which concentrated on threats.

ROEs

Almost all CGF programs have three ROEs (Hold Fire, Fire if Fired Upon, and Fire at Will). Subject Matter Experts indicated that in Small Scale Contingency (SSC) and Force Protection missions, there is a fourth ROE (Fire On Hostile Intent). The definition of hostile intent is dependent on the situation. For dismounted infantry and civilians, having a deployed fire arm is not hostile intent but aiming it at a friendly is hostile intent. Brandishing a knife is not hostile intent. Crashing through an entry control point with a vehicle is hostile intent with or without a weapon displayed. Implementing this additional ROE required an additional state along with the set of rules for determining when behavior indicative of hostile intent has occurred.

Usability

SF instructors predicted that the SecForDMT technology would be more valuable when training for mission planning than when training for mission execution. This is because decision-makers have more impact on the success of a mission through the decisions they make during mission planning than from the decisions made during the few minutes of an engagement. In air base defense, officers are given a sector of responsibility and resources (personnel, weapons, sensors and barriers) to use in defending that sector. They then study the vulnerability and value of the assets to be protected, intelligence reports on likely threats, topography of the sector, and proximity of host nation citizens. They then plan their defenses and document the proposed locations of resources on a map of the sector.

We have developed a plan view display with capabilities for officers and squad leaders to position resources in the same manner they would use in the planning process. Figure 3 is the SecForDMT plan view display with resources in place for a base defense.

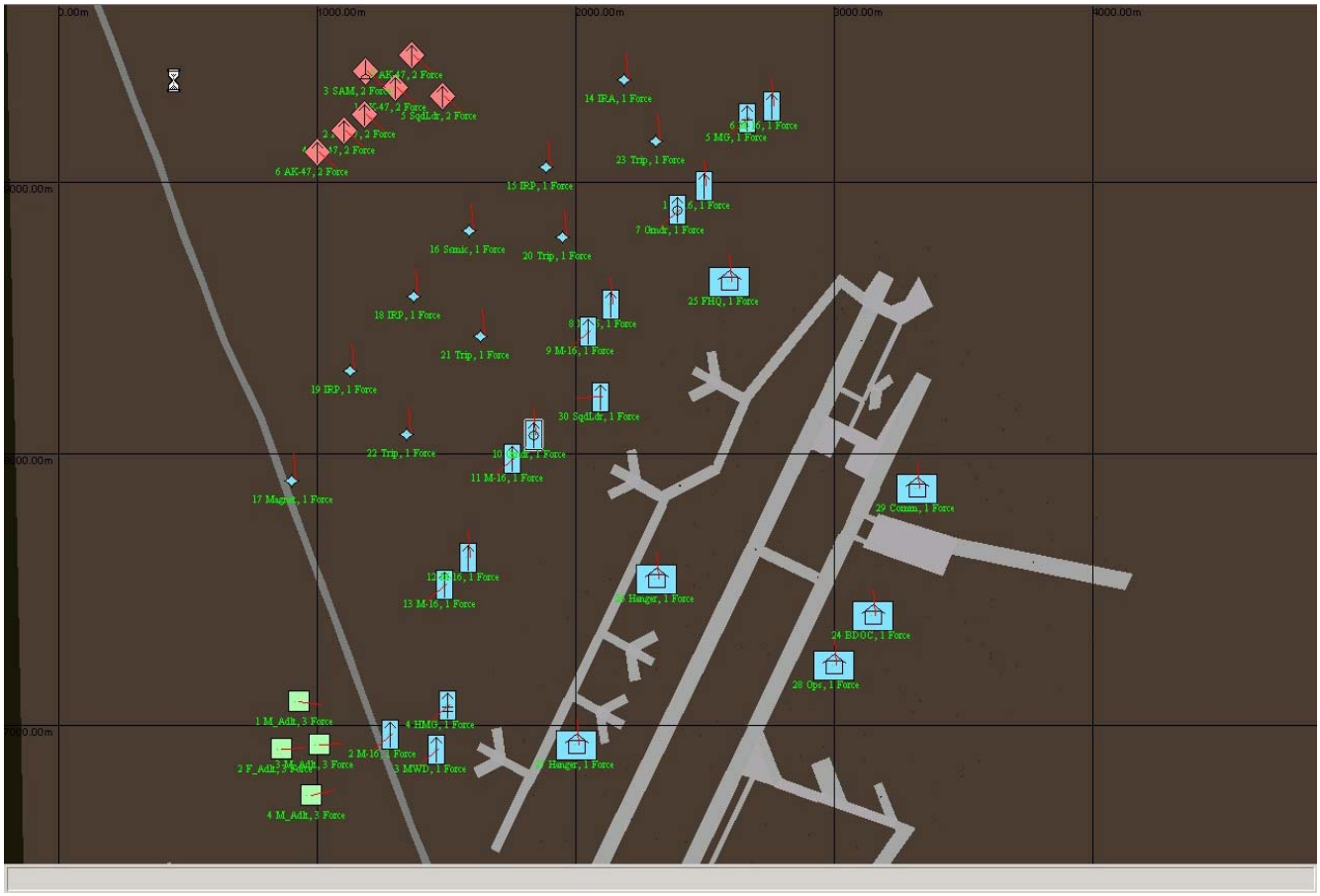

Figure 3
Sample SecForDMT Plan View Display

The rectangles represent fighting positions and the arrow symbols represent security forces with various weapons. The arrow with a cross hatch is a dismounted infantry SF with an M-60 machine gun. These symbols are based on MIL-STD 2525B and FM 101-5-1/MCRP 5-2A. These are the same symbols currently used by security forces in designating the locations of resources on paper planning maps. ModSAF chose to represent dismounted infantry on their plan view display with icons that looked like an overhead view of soldiers in various postures. In SecForDMT we chose to use these standard weapons symbols because the planners are more interested in the type of weapons carried than in the posture of the soldier.

As planners select these resources via menu selection and place them on the PVD with the mouse, they are inserting them into the virtual world at that location. Rules of engagement and movement plans can be assigned to entities by clicking on the symbol and editing the unit plan. These resources are then saved in a scenario for later execution.

Stealth Display

Figure 4 contains a sample image from the stealth display. We are using a commercially available stealth display. However, this display did not originally have dismounted infantry and neutrals in its image files. These dismounted infantry and neutral characters were developed on the SecForDMT project. As indicated above, we are not certain whether the increased cost of a stealth display is justified in a decision-making trainer. We plan to evaluate the cost effectiveness of the stealth display for SecForDMT technology in later phases of the project.

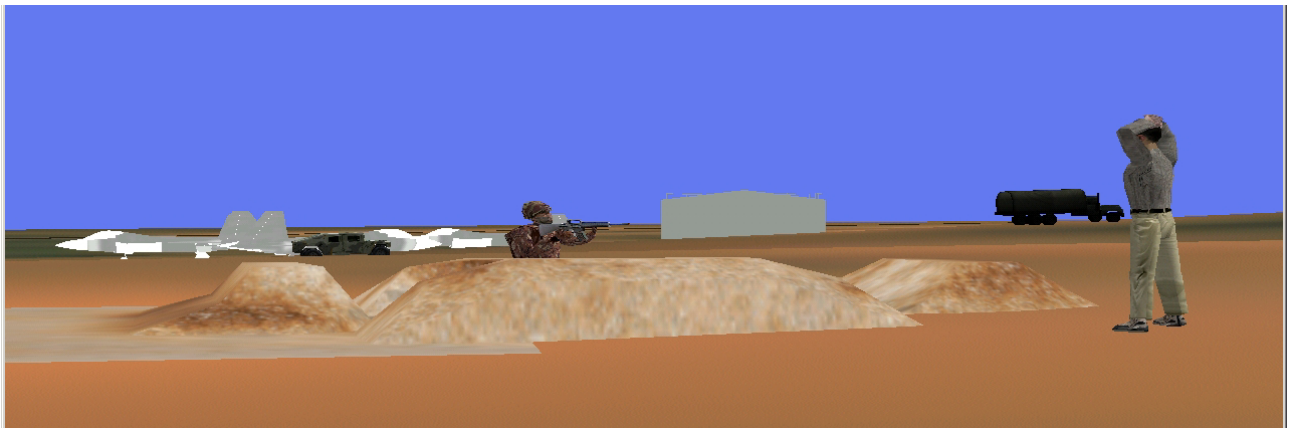

Figure 4
Sample Stealth Image

Multipurpose Behavior Models
We had mixed success in developing generic behavior that could be used by a number of different types of CGFs. At first, we attempted to model behavior of security forces under only two conditions, moving and stationary. However, further analyses indicated that appropriate behaviors at an Entry Control Point (where many friendly and neutral individuals and vehicles are anticipated) are substantially different from appropriate behaviors at a fighting position (where few friendlies and no neutrals are anticipated). We also tried to model generic aggressiveness across friendly, neutral and threat CGFs. However, aggressive behavior from unarmed neutrals, armed neutrals, armed threats and armed friendlies are substantially different. We were able to have some code serve multiple purposes, but not as much as we had hoped.

Communications Protocol
Since one of the primary goals of SecForDMT technology development is to reinforce correct communications protocol, our CGFs must issue SPOT reports using the SALUTE (size, activity, location, unit, time, and equipment) format. A typical SPOT reports in SecForDMT is shown below:

> Red Dog 1, This is Red Dog 1,5
> There are five dismounted infantry moving at approximately four kilometers per hour across my sector on a heading of approximately 30 degrees at grid location 59114688. They are using cover and concealment. These are threat forces. Time of observation 0935 Zulu. They are carrying small arms.

The creation of this SPOT report requires the grouping of individual entities into tactical groups, counting entities in the group, reading the velocity vector and other state information about the approaching CGFs, reading the Force ID and constructing SPOT reports. Since SPOT reports serve as the key information source for the SF trainees, substantial effort was applied to developing this capability. A similar approach is being applied to the LACE (liquid, ammunition, casualties and equipment) report at the end of each engagement.

Initial Evaluation

The authors conducted an initial evaluation of the SecForDMT tool with 14 instructors at the Desert Warfare Training Center at Nellis AFB in Nevada. The officers were a Captain with Air Base defense (ABD) experience and a Lieutenant with training but no experience. The enlisted personnel ranged from SSgt. to Senior MSgt. with substantial experience. All of the evaluators were very enthusiastic about the usefulness of the tool in helping trainees understand and demonstrate their understanding of ABD. In addition to being a valuable tool for conducting exercises in a distributed mode, they believed the tool would also allow trainees to prepare ABD plans at home station and email them in for instructor critique and correction before implementing real-time distributed training exercises. They also believed that students could use the computer generated OPFOR to learn of weaknesses in their plans before submitting them to the instructors.

In critiquing the developmental tool, they pointed out that SITREPs generated by the CGFs were more detailed than they teach their trainees. For example, SecForDMT CGFs report approaching threats based on a Military Grid Reference eight digit coordinate system as described in the Field Manuals. The Air Force uses a simpler approach of reporting bearing and range to

target. Also, their reports of target speed are walking, SecForDMT CGFs are currently being modified to report in the manner taught by the instructors.

Finally, the instructors viewed exercises using both a Plan View Display (PVD) and a stealth display. The great majority of instructors felt that the stealth display added a great deal of pizzazz to the program but had limited training value. This would stand to reason because SecForDMT technology supports command and control training as opposed to first person shooter training. Most decision-makers make heavy use of maps during planning and monitoring operations based on SITREPs. Consequently, they feel comfortable using a PVD.

Conclusions

Based on results of the first phase, it appears that a simulation can be developed with sufficient affordability, validity and usability to provide effective distributed mission training to Air Force security forces decision-makers for SSC force protection. While the nuances of applying SSC force protection ROEs make the CGF development process more challenging, it appears that the technical hurdles can be overcome.

Lessons Learned

In addition to the successes and problems discussed above, there were a number of lessons learned on Phase 1 of the project:

- After reviewing manuals, it would appear that CGF behaviors in air base defense scenarios would be straightforward. However, the required behavior becomes much more complex after interviewing SMEs about appropriate behavior for each combination of mission assignment, ROE, threat behavior and actions of neutrals. Then when the behavior is being tested, many conditions not even envisioned by the SMEs arise that require even more subtle behaviors.
- Procedures that could easily be followed by humans lead to problems when implemented by CGFs. These problems do not become apparent until testing with realistic scenarios. In order to create credible behavior, the developers must add additional details that cover nearly every possible variation in environment and other CGF behaviors. Although tedious, we found the If-Then paradigm adequate to create these behaviors.
- Force protection behavior in SSCs is considerably more complex than cold war behavior and the CGFs must exhibit behavior that exhibits the nuances and subtleties in the environment and behaviors of other CGFs.

crawling or running as opposed to X kph. The

Future Plans

Now that the fixed base defense behaviors have been developed and tested, the next phase will concentrate on patrols and convoys. We will also begin implementing and testing Internet communications and addressing problems anticipated with limited bandwidths.

References

McDonald, L.B., Weeks, J., & Harris, T. (2000). Security forces distributed mission training technology development. Proceedings of the 2000 Fall Simulation Interoperability Workshop, Orlando, FL.

Pew, R., & Mavor, A., (1998). Modeling human and organizational behavior: Applications to military simulations. Washington DC: National Academy Press.

Shlapak, D. & Vick, A. (1995). Check Six begins on the ground: Responding the evolving ground threat to U.S. Air Force bases (Report MR-606-AF). Santa Monica CA: Rand Corp.

U.S. Air Force Instruction 31-301 (August 1996). Air Base Defense.

U.S. Air Force Handbook 31-302 (January 1996). Air Base Defense Collective Skills.

U. S. Air Force Personnel Center (May 2001). Personnel Statistics. Generated by Joseph Weeks; using the Interactive Demographic Analysis System http://www.afpc.randolph.af.mil/vbin/broker8.exe

U.S. Army Field Manual 7-8 (1 March 2001). Infantry Rifle Platoon and Squad, Change 1.

U.S. Army Field Manual 101-5-1/MCRP 5-2A (1997).- Operational Terms and Graphics.

U. S. Department of the Air Force, Headquarters United States Air Force (2001). AFSC 31P1/3/4, Security Forces Officer Specialty, Career Field Education and Training Plan. Washington DC.

U.S. DoD (1999). MIL-STD 2525B, Standard Warfighting Symbology.

Vick, A. (1995). Snakes in the eagle's nest: A history of ground attacks on air bases (MR-553-AF). Santa Monica, CA: Rand Corp.

Weeks, J., Garza, J., Archuleta, M., & McDonald, B., (Nov 2001). USAF security forces training needs. Proceedings of the 12th Interservice/ Industry Training Systems Conference, Orlando, FL.